AF/2132

#21/2700

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	James Q. Mi, et al.	§	Group Art Unit:	2132
		§		
Serial No.:	09/259,620	§		
		§	Examiner:	Douglas J. Meislahn
Filed:	February 26, 1999	§		
		§		
For:	COMPUTER SYSTEM IDENTIFICATION	§	Atty. Dkt. No.:	ITL.0160US
		§		

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

REPLY BRIEF

Dear Sir:

The following reply is submitted to the Examiner's Answer.

I. CLAIMS APPEALED

The appealed claims are claims 1, 3-5, 21 and 22 grouped together; claims 6, 8, 9, 23 and 24 grouped together; claims 10-14, 25 and 26 grouped together; claims 15-20 grouped together; claims 27-30 grouped together; claims 31-34 grouped together; and claims 35-38 grouped together.

Date of Deposit: December 8, 2003
I hereby certify under 37 CFR 1.8(a) that this correspondence is being deposited with the United States Postal Service as **first class mail** with sufficient postage on the date indicated above and is addressed to the Commissioner for Patents, P.O. Box 1450,, Alexandria, Virginia 22313-1450.

Janice Munoz

Janice Munoz

II. REPLY TO EXAMINER'S ARGUMENTS

A. Can claims 1, 3-5, 21 and 22 be rendered obvious when the Examiner has failed to establish a *prima facie* case of obviousness for independent claim 1?

From the Examiner's Answer, it appears that the Examiner is at least implicitly contending that the user personal identification number (PIN) of Claus identifies Claus's smart card. Examiner's Answer, 10. However, as Applicant has previously pointed out, the PIN of Claus identifies the user of the card, as the security technique disclosed in Claus is directed to securing the stored user information. For example, suppose a smart card manufacturer manufactures a thousand smart cards. Claus is not concerned as to which one of those cards makes it to the end user. Rather, once one of these cards is associated with a particular user, this smart card is then secured so that the PIN of the user is required to access the card. The PIN of Claus does not reveal the identity of the smart card (out of the one thousand smart cards for this example). Thus, the PIN of Claus identifies a smart card user, not the smart card and not a processor of the smart card.

Thus, the Examiner relies on the combination of Claus and Lee for the § 103 rejection of independent claim 1. However, the Examiner still fails to show where the prior art contains the alleged motivation or suggestion to modify Claus in view of Lee to derive the claimed invention.

More specifically, in attempt to show the alleged suggestion or motivation, the Examiner cites language from lines 12-23 of column 1 of Lee. This language states that a serial number "allows the manufacturer greater control over its product." Lee, 1:17-18. Thus, there may be a suggestion or motivation in the prior art to modify Claus's smart card so that this smart card has a processor number for purposes of allowing the smart card manufacturer greater control over its product. However, even assuming, *arguendo*, that this modification is proper, the Examiner still fails to show the alleged suggestion or motivation to modify Claus so that Claus's PIN is replaced with such a processor number. In other words, why would one skilled in the art had modified Claus in view of Lee so that the encryption and hashing disclosed in Clause are applied to a processor number that identifies a processor of the smart card? At best, the combination of Lee and Claus produces a smart card that encrypts a user PIN (as set forth in Claus) and includes a processor number. However, the Examiner fails to show the required suggestion or motivation in the art to derive the claimed invention and thus, establish a *prima facie* case of obviousness, i.e., the Examiner fails to show where the prior art contains the alleged suggestion or motivation to modify Claus in view of Lee so that the smart card of Claus encrypts Lee's processor number to produce a hash value in response to an identification request.

Thus, the Examiner fails to establish a *prima facie* case of obviousness for claims 1, 3-5, 21 and 22; and the § 103 rejections of these claims should be reversed.

B. Can claims 6, 8, 9, 23 and 24 be rendered obvious when the Examiner has failed to establish a *prima facie* case of obviousness for independent claim 6?

See reply to Issue A above. The Examiner fails to show where the prior art contains the alleged suggestion or motivation to modify Claus in view of Lee so that a processor of Claus's smart card encrypts a processor number that identifies the processor with a key that is associated with a computer system. Simply placing a processor number on Claus's smart card (in view of the language of Lee cited by the Examiner) in view of Lee does not teach or suggest the above-recited limitations of independent claim 6.

Thus, the Examiner fails to establish a *prima facie* case of obviousness for claims 6, 8, 9, 23 and 24; and the § 103 rejections of these claims should be reversed.

C. Can claims 10-14, 25 and 26 be rendered obvious when the Examiner has failed to establish a *prima facie* case of obviousness for independent claim 10?

Zdepski teaches a direct broadcast satellite system that includes a subscriber platform 145 and a database server 276. Zdepski describes that for a communication from the subscriber platform 145 to the database server 276, the subscriber platform 145 encrypts a subscriber identification with a "database server public key". Zdepski, 4:64-67. Schneier discloses a public key certificate that is used to thwart an attempt to substitute one public key for another. Schneier, 185.

The article of claim 10 includes instructions that cause a processor to receive a key from another processor-based system that identifies this other processor-based system, determine whether the key is valid, and based on the identification, selectively authorize encryption of an identifier that identifies the first system.

The Examiner merely assumes that the database server public key of Zdepski is received from the database server 276. Examiner's Answer, 6-7. However, such an assumption is improper, as this teaching does not necessarily flow from Zdepski. To the contrary, the database public key could have been received from other sources. For example, this key could be preprogrammed into the subscriber system, could be furnished by a system other than the database server, could be furnished by an access card that is inserted into the subscriber platform, etc. Thus, even assuming, *arguendo*, that the combination of Zdepski and Schneier is proper, the combination of references fails to teach or suggest all limitations of independent claim 10, such as instructions to cause a processor to receive a key from another processor-based system for identifying that other system.

Thus, the Examiner fails to establish a *prima facie* case of obviousness for claims 10-14, 25 and 26; and the § 103 rejections of these claims should be reversed.

D. Can claims 15-20 be rendered obvious when the Examiner has failed to establish a *prima facie* case of obviousness for independent claim 15?

The Examiner continues to ignore claim limitations that explicitly appear in independent claim 15 and without even addressing Applicant's points concludes that Applicant's arguments "are unpersuasive." Examiner's Answer, 12-13.

However, contrary to the Examiner's position, the Examiner fails to show where the prior art teaches or suggests all claim limitations and thus, fails to establish a *prima facie* case of obviousness for claims 15-20. As yet another example of a missing claim limitation, the microprocessor of claim 15 includes an instruction unit that is adapted to indicate when the instruction unit receives an instruction that requests an identifier that identifies the microprocessor.

Neither Claus nor Schneier teaches or suggests an identifier that identifiers a microprocessor.

Furthermore, even assuming, *arguendo*, that the combination of Claus and Schneier teaches such an identifier, neither reference teaches or suggests an instruction unit that is adapted to indicate when the instruction unit *receives an instruction that requests the identifier*. It appears the Examiner is contending that these missing claim limitations are somehow inherent in Claus. However, for a missing claim limitation to be inherent in a reference, the missing claim limitation must *necessarily flow* from the reference. *Ex parte Levy*, 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter. 1990). This is not the case here, as clear alternatives exist. For example, it is not necessary that an instruction unit of a microprocessor receive a dedicated instruction for requesting the identity of the microprocessor. Instead, the microprocessor could execute other instructions related to reading, writing and mathematically manipulating data without the existence of such a specific instruction. Therefore, as clear alternatives exists, the missing claims limitations do not necessarily flow from either of the cited references.

Thus, the Examiner fails to establish a *prima facie* case of obviousness for claims 15-20; and the § 103 rejections of these claims should be reversed.

E. Can claims 27-30 be rendered obvious when the Examiner has failed to establish a *prima facie* case of obviousness for independent claim 27?

Claus fails to teach or suggest using a hash value to identify information that is stored in a first computer system and is associated with a user of a second computer system. More particularly, the Examiner labels Claus's smart card as the alleged second computer system and labels Claus's authentication device as the alleged first computer system of claim 1. Thus, the question becomes whether Claus teaches using a hash value to identify information that is stored in the authentication device and is associated with a user of the smart card.

Contrary to the Examiner's contentions, Claus fails to teach or suggest using a hash value (associated with a user of the smart card) to identify information that is stored in the authentication device. The Examiner cites to language in columns 1 and 3 of Claus. Examiner's Answer, 13. However, the language cited from column 1 makes a general reference to cryptosystems; and the language cited from column 3 states, "the present invention eliminates the need to store and administer identification information regarding each user entitled to access to the protected resources." Applicant submits that neither passage teaches nor suggests the missing claim limitations.

Thus, the Examiner fails to establish a *prima facie* case of obviousness for claims 27-30; and the § 103 rejections of these claims should be reversed.

F. Can claims 31-34 be rendered obvious when the Examiner has failed to establish a *prima facie* case of obviousness for independent claim 31?

For at least the reasons set forth above in the discussion of Issue E, the Examiner fails to show where Claus teaches or suggests using a hash value to identify information that is stored in a first computer system and is associated with a user of a second computer system.

Thus, the Examiner fails to establish a *prima facie* case of obviousness for claims 31-34; and the § 103 rejections of these claims should be reversed.

G. Can claims 35-38 be rendered obvious when the Examiner has failed to establish a *prima facie* case of obviousness for independent claim 35?

For at least the reasons set forth above in the discussion of Issue E, the Examiner fails to show where Claus teaches or suggests a first computer to use a hash value to identify information that is stored in a database and is associated with a user of a second computer system. The Examiner does not specifically address the elements of claim 35, i.e., the first computer and the database. Furthermore, the Examiner fails to identify the alleged second computer in the prior art.

Thus, the Examiner fails to establish a *prima facie* case of obviousness for claims 35-38; and the § 103 rejections of these claims should be reversed.

III. CONCLUSION

Applicant requests that each of the final rejections be reversed and that the claims subject to this appeal be allowed to issue. The Commissioner is authorized to charge any fees or credit any overpayment to Deposit Account No. 20-1504 (ITL.0160US).

Respectfully submitted,

Date: December 8, 2003

Fred G. Pruner, Jr., Reg. No. 40,779
TROP, PRUNER & HU, P.C.
8554 Katy Freeway, Suite 100
Houston, TX 77024-1805
713/468-8880 [Phone]
713/468-8883 [Facsimile]

APPENDIX OF CLAIMS

The claims on appeal are:

1. A method comprising:

receiving a request from a first computer system for identification of a second computer system;

retrieving a processor number that identifies a processor of the second computer system;

encrypting the processor number with a key associated with the first computer system to produce a hash value; and

providing the hash value to the first computer system in response to the request.

3. The method of claim 1, further comprising:

executing a processor instruction; and

retrieving the number in response to the execution of the instruction.

4. The method of claim 1, further comprising:

receiving the key from the first computer system.

5. The method of claim 1, wherein the key indicates an address of a web site.

6. An apparatus comprising:

an interface adapted to:

receive a request from a computer system for identification of the apparatus, and

furnish a hash value that identifies the apparatus to the computer system; and

a processor coupled to the interface and adapted to:

encrypt a processor number that identifies the processor with a key associated with the computer system to produce the hash value.

8. The apparatus of claim 6, wherein the processor comprises:

a memory adapted to store microcode for performing the encryption; and

a control unit coupled to the memory and adapted to execute the microcode to perform the encryption.

9. The apparatus of claim 6, wherein the processor is further adapted to: interact with the interface to receive the key from the computer system.

10. An article comprising a storage medium readable by a first processor-based system, the storage medium storing instructions to cause a processor to:

receive a key from another processor-based system for identifying said another processor-based system,

determine whether the key is valid,

based on the identification, selectively authorize encryption of an identifier that identifies the first system with the key to produce a hash value.

11. The article of claim 10, the storage medium storing instructions to cause the processor to:

use an address of said another system to determine whether the key is valid.

12. The article of claim 11, wherein the key indicates an URL address.

13. The article of claim 10, the storage medium storing instructions to cause the processor to:

execute an instruction to cause the processor to subsequently use the key to produce the hash value.

14. The article of claim 10, wherein the identifier comprises a processor number.

15. A microprocessor comprising:

an instruction unit adapted to indicate when the instruction unit receives an instruction that requests an identifier that identifies the microprocessor;

an execution unit coupled to the instruction unit and adapted to, in response to the indication from the instruction unit, encrypt a key with the identifier to produce a hash value; and a bus interface unit coupled to the execution unit and adapted to furnish an indication of the hash value to external pins of the microprocessor.

16. The microprocessor of claim 15, wherein the execution unit comprises:

a control unit; and

a memory coupled to the control unit and storing microcode to cause the control unit to use the key and the identifier to produce the hash value.

17. The microprocessor of claim 15, wherein the identifier comprises a processor number.

18. The microprocessor of claim 15, wherein the execution unit is adapted to use a one way hash function to produce the hash value.

19. The microprocessor claim 15, wherein the execution unit is adapted to use a non-commutative hash function to produce the hash value.

20. The microprocessor of claim 15, wherein the execution unit is adapted to use a collision free hash function to produce the hash value.

21. The method of claim 1, wherein the processor number identifies a microprocessor of the second computer system.

22. The method of claim 21, wherein the processor number uniquely identifies the microprocessor.

23. The computer system of claim 6, wherein the processor number identifies a microprocessor of the apparatus.

24. The computer system of claim 23, wherein the processor number uniquely identifies the microprocessor.

25. The article of claim 14, wherein the processor number identifies a microprocessor of the first system.

26. The article of claim 25, wherein the processor number uniquely identifies the microprocessor.

27. A method comprising:

providing a request to a second computer system for the second computer system to provide an identification of the second computer system;

receiving a hash value from the second computer system, the hash value being generated by encryption of a key associated with a first computer system with an identifier that identifies the second computer system; and

using the hash value to identify information associated with a user of the second computer system, the information being stored in a database maintained by the first computer system.

28. The method of claim 27, wherein the identifier that identifies the second computer system comprises a processor number.

29. The method of claim 27, wherein the key indicates an address of a web site of the first computer system.

30. The method of claim 27, wherein the first computer system is located at a remote location relative to the second computer system.

31. An article comprising a storage medium readable by a first processor-based system, the storage medium storing instructions to cause a processor of the first processor-based computer system to:

provide a request to a second computer system for the second computer system to provide an identification of the second computer system;

receive a hash value from the second computer system, the hash value being generated by encryption of a key associated with the first computer system with an identifier that identifies the second computer system; and

using the hash value to identify information associated with a user of the second computer system, the information being stored in a database maintained by the first computer system.

32. The article of claim 31, wherein the identifier that identifies the second computer system comprises a processor number.

33. The article of claim 31, wherein the key indicates an address of a web site of the first computer system.

34. The article of claim 31, wherein the first computer system is located at a remote location relative to the second computer system.

35. A system comprising:

a database; and

a first computer coupled to the database to:

provide a request to a second computer for the second computer to provide an identification of the second computer,

receive a hash value from the second computer, the hash value being generated by encryption of a key associated with the first computer with an identifier that identifies the second computer, and

use the hash value to identify information associated with a user of the second computer, the information being stored in the database.

36. The system of claim 35, wherein the identifier that identifies the second computer comprises a processor number.

37. The system of claim 35, wherein the key indicates an address of a web site of the first computer.

38. The system of claim 35, wherein the first computer is located at a remote location relative to the second computer.